*Agency Name*_____ *Date*_____

This document must be completed by the Agency to demonstrate compliance status with the Payment Card Industry Data Security Standard (PCI DSS) and Visa Operating Regulations requirements prohibiting the storage of sensitive cardholder account authentication information beyond authorization.

☐ No evidence of magnetic stripe (i.e., track) data[1], CVV2[2] data, or PIN data[3] were found subsequent to transaction authorization on ANY systems reviewed during this assessment.

☐ Magnetic stripe (i.e., track) data, CVV2 data, or PIN data are retained on systems subsequent to transaction authorization. Remediation plans and timelines for addressing the issue are attached.

X _____

(Signature of authorized agent for the above Agency) *(Date)*

X _____

(Printed Name) *(Title)*

*Email address*_____

[1] Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data subsequent to transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.
[2] CVV2 – The three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions.
[3] PIN Data – Personal Identification Number entered by cardholder during a card-present transaction and/or encrypted PIN block present within the transaction message.

Treasurer's Office Use Only

Merchant Level:
(check one)

☐ **Level 1** ☐ **Level 2** ☐ **Level 3** ☐ **Level 4**

Merchant confirms:
(check all that apply):